TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI
2€
NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI
n. 168
HACKER JOURNAL
www.hackerjournal.it
HACKER TEST
24 ORE CACCIANDO RETI WIFI
HACKING GAMES
TUTTI I BUG DI
PLAYSTATION HOME
WINDOWS LIVE MESSENGER
COME TI RUBO
L'ACCOUNT
PROGRAMMING
METTI IN SICUREZZA
IL TUO SITO
GOOGLE PHONE
PRESENTATO...
HACKERATO
QUATTORD. ANNO 9 - N° 168 - 22 GENNAIO/4 FEBBRAIO 2009 - € 2,00
WLF PUBLISHING

Anno 9 – N.168
22 gennaio/4 febbraio 2009

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

La dottoressa Meg

"L'ignoranza è temporanea, la stupidità è per sempre".
Anonimo

L'università del Wisconsin-Madison ha mandato a centinaia di utenti MySpace una semplice mail con il seguente messaggio: «Sei sicuro che si tratti di una buona idea parlare così apertamente delle tue abitudini sessuali o dell'abuso di alcol, fumo e droga? Non sarebbe meglio proteggere meglio la tua privacy?». Firmato dottoressa Meg.

E fin qui l'unica domanda che viene in mente è perché la dottoressa Megan Moreno (Meg) non si faccia i fatti suoi...

Poi viene fuori che si tratta di un esperimento e che il 42% delle persone che hanno ricevuto la mail ha modificato le proprie impostazioni, tutelando maggiormente i dati personali, o ha addirittura rimosso certe informazioni. Ma il dato davvero sconfortante è che molti ragazzi hanno risposto alla dottoressa Meg spiegando di non sapere che le proprie pagine potessero essere visualizzate da chiunque, in qualunque parte del mondo.

Questa, che può sembrare una storiella da inizio anno nuovo in realtà deve far riflettere, e molto.

Io e i miei colleghi, come immagino tu che stai leggendo, siamo ormai abituati a considerare sempre gli aspetti relativi alla sicurezza e alla privacy in tutto ciò che facciamo. Deformazione professionale. Pensare però che centinaia di ragazzi iscritti a un social network non sapessero che le informazioni potessero essere visualizzate da chiunque in tutto il mondo ridisegna completamente i confini di ciò che è privacy e ciò che intendiamo per sicurezza. Non si tratta più di combattere con persone senza scrupoli che vogliono rubarci informazioni sensibili o usare il nostro computer per attacchi di massa, qui si tratta di far capire alle persone che non c'è antivirus o firewall che tenga se poi le nostre informazioni riservate le mettiamo a disposizione di tutti su un social network.

Proposito per l'anno nuovo:

Spiega ai tuoi amici che fare parte della grande comunità di Facebook & Co è bello, ma che esistono cose più intelligenti che comunicare al mondo (e quindi ai propri insegnanti o ai datori di lavoro) che ci si droga o si beve troppo. Ti sembra improbabile? Lo faceva il 41 % degli scritti a MySpace.

The Guilty

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa!
Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Internet Explorer, patch da record

L'ultimo patch-day di Microsoft è arrivato ed è passato, come al solito, in tutta tranquillità. Si è fatto attendere un po' di più, ma la mole di patch e aggiornamenti in effetti è stata abbastanza ampia da richiedere qualche giorno in più per la localizzazione e la messa a punto. Sembrava tutto passato, ma il giorno dopo è stato pubblicato sul Web un exploit contro Internet Explorer che, mediante una tecnica di SQL Injection, avrebbe permesso di eseguire codice con privilegi di amministratore su tutte le macchine online su cui fosse stato in funzione il browser di Microsoft visitando un sito maligno appositamente progettato.

La gravità della cosa è apparsa subito notevole, per diversi aspetti. Innanzitutto, chi ha scoperto la falla di sicurezza si è premurato di pubblicarla anche sul Web, a uso e consumo di qualunque malintenzionato passasse da quelle parti. In secondo luogo, detta falla non affliggeva solamente una determinata versione del browser, ma tutte le versioni a partire dalla 5 in poi, compresa la beta di Internet Explorer 8, allargando a dismisura il pericolo di ricevere un attacco. Infine, la tempestività con cui è stata resa nota la vulnerabilità fa pensare che i cracker più incalliti abbiano messo a punto una nuova tattica, quella di aspettare pazientemente il patch-day per ottenere due vantaggi: primo, la possibilità di agire con nuovi exploit quando i giochi sono chiusi e ci vorrà tempo per preparare nuove eventuali patch; secondo, dopo un aggiornamento si può in tutta tranquillità effettuare il reverse engineering delle patch per preparare attacchi sfruttando falle non conosciute (ma scoperte da Microsoft) e l'ingenuità di chi non tiene il proprio sistema aggiornato.

Quanto è successo con Internet Explorer nell'ultimo periodo, però, ha aiutato Microsoft ad affinare anche le proprie tecniche di difesa, scoprendo la nuova tendenza dei cracker ad agire subito dopo il rilascio di un aggiornamento. Ogni vulnerabilità sfruttata da un cracker costituisce un utile precedente, per Microsoft, per scovare e rimediare a eventuali altre falle dello stesso tipo, riuscendo a prevenire prima di curare. Il che, detto tra noi, avrebbe dovuto essere la filosofia di base di Microsoft sin dagli albori, dalle prime versioni dei propri prodotti, anziché un obiettivo da raggiungere dopo aver "perso tempo" per anni a rattoppare del codice che, lo dimostrano avvenimenti come quello accennato in queste righe, è tutto fuorché ben progettato e sicuro.

Diamo atto comunque alla casa di Redmond di aver migliorato di molto il livello di usabilità e di affidabilità del sistema di aggiornamento: la patch per Internet Explorer che ha corretto il problema qui presentato si è fatta attendere "solo" otto giorni, davvero un tempo record rispetto a quelli biblici che abbiamo riscontrato in passato.

SVENDO MP3 USATI!

Da Bopaboo arriva un'idea, se non originale poco ci manca: la vendita online di MP3 usati. Si tratta di un esperimento commerciale che permette agli utenti di mettere a disposizione i propri MP3, rigorosamente senza DRM, per essere rivenduti online. Naturalmente questo nuovo servizio non ha mancato di suscitare clamore, dato che si parla di musica e di diritti: secondo alcuni è illegale, perché permetterebbe di rivendere brani acquistati legalmente rientrando così della spesa e mantenendo una copia degli stessi; secondo altri invece la rivendita di materiale digitale ricade nei diritti di qualunque utente. La diatriba quindi è aperta, ma per ora il sito www.bopaboo.com risulta aperto solo per utenti risiedenti negli Stati Uniti. Non resta che aspettare gli sviluppi.

bopaboo beta

2008! IL BISESTO PIU' LUNGO

L'hanno riportato anche i telegiornali la sera del 31 dicembre e così hanno fatto a Capodanno: il 2008 è durato un secondo di più del normale. L'ultimo minuto dello scorso anno è stato convenzionalmente allungato di un secondo, durando quindi 61 secondi invece di 60, per compensare la differenza tra l'orario fisico dovuto alla rotazione terrestre con quello misurato dagli orologi atomici. Questa differenza è dovuta alle lievissime fluttuazioni che subisce il percorso della Terra nello spazio e che ne modificano la rotazione. Il risultato è, anche se non ce ne siamo resi conto in preda all'euforia dei festeggiamenti, è che per un secondo in più siamo rimasti nel vecchio anno, come stabilito dall'International Earth Rotation and Reference Systems Service, l'ente che si occupa di regolare il Tempo Universale Coordinato (UTC).

EUROPEANA DI NUOVO ONLINE

Aveva aperto il portale sul Web il 20 novembre scorso ma aveva chiuso subito dopo a causa dell'enorme quantità di accessi ricevuta, che aveva causato problemi al servizio. Ora il sito di Europeana, la biblioteca virtuale europea che promette l'accesso a 2 milioni di oggetti digitali (tra cui immagini, video, suoni e testi), è di nuovo online ma con funzionalità ridotte nelle ore di punta. Si sta provando una nuova implementazione hardware, così dice la home page del sito (http://www.europeana.eu/portal/), e pertanto il servizio potrebbe non essere affidabile al 100%. Speriamo sinceramente che tutti i problemi hardware si risolvano: avere una valida alternativa a Google e Wikipedia in ambito europeo non è un'idea malvagia, soprattutto per quelli di noi che ancora passano il proprio tempo studiando sui libri di scuola.

TORRENT BATTE MICROSOFT

Forse Microsoft voleva mantenere il riserbo più a lungo, a proposito di Windows 7 e delle sue caratteristiche. Aveva rilasciato una pre-beta solo per gli sviluppatori per potersi adeguare ai nuovi standard; fatto sta che ancora una volta i canali di distribuzione non ufficiali hanno battuto sul tempo il produttore: Windows 7 ha già fatto la sua comparsa nei canali peer to peer grazie a un torrent messo a disposizione da qualcuno che lo ha avuto per mezzo dei canali regolari. A parte le considerazioni etiche, chi ha scaricato il torrent e ha provato a installare il nuovo sistema operativo ne è rimasto piacevolmente impressionato, sia per quanto riguarda la velocità in generale dell'installazione e del sistema stesso, sia per quanto riguarda le nuove caratteristiche.

FENNEC ALPHA 2

Mozilla ha recentemente rilasciato una nuova pre-release del browser per dispositivi mobili Fennec. Questa alpha 2 è disponibile per Windows, Linux, Mac OS e per la piattaforma Nokia N810, ma non è ancora pronta per essere installata su dispositivi Windows Mobile 6.1 (forse la piattaforma che più delle altre lo attende). Tra le funzionalità presentate, la capacità di riconoscere i numeri di telefono inseriti nelle pagine Web e di permettere la chiamata rapida a quello selezionato (ottimo, dato che è un software per smartphone) e la presenza di tecnologie di geolocalizzazione. Inoltre sono state migliorate la visualizzazione delle pagine e la possibilità di ingrandire i contenuti, sempre utile in display minuscoli. Per scaricare questa versione alpha 2 si può visitare l'indirizzo http://www.mozilla.org/projects/fennec/1.0a2/releasenotes/.

DJ SENZA LICENZA

Sul Web si sta sollevando una questione delicata, per far sentire al pubblico, ma soprattutto a chi di dovere, la voce delle migliaia di DJ che operano in Italia. Infatti i DJ sono costretti per causa di forza maggiore a violare la legge sui diritti d'autore di continuo: pur possedendo regolarmente i supporti originali dei brani che usano nelle loro esibizioni, non possono legalmente sfruttare i vantaggi delle nuove tecnologie, come il trasferimento in MP3 dei brani per un trasporto più semplice o l'esecuzione di copie di lavoro per preservare i CD originali durante le movimentate serate. Il tutto è causato principalmente dalle estenuanti pratiche burocratiche imposte dalla SIAE e dai vincoli imposti dalle leggi sul diritto d'autore, che ogni volta devono essere aggirati inventandosi sempre nuovi escamotage per poter lavorare.

SQL Server fallato

Microsoft ha emanato un comunicato ufficiale in cui informa che SQL Server 2000, SQL Server 2005 e 2005 Express Edition, SQL Server 2000 Desktop Engine e Windows Internal Database sono affette da un problema di sicurezza. Si tratta di una stored procedure, sp_replwritetovarbin, che permetterebbe a un aggressore di eseguire codice maligno sfruttando i privilegi del processo in uso. Nel comunicato Microsoft conferma che SQL Server 7.0 SP 4, SQL Server 2005 SP 3 e SQL Server 2008 non sono influenzate dalla falla di sicurezza, che nelle altre versioni può essere arginata accedendo alla console di amministrazione del server e impartendo i comandi use master e deny execute on sp_replwritetovarbin to public. All'indirizzo http://www.microsoft.com/technet/security/advisory/961040.mspx si può trovare il bollettino ufficiale di Microsoft.

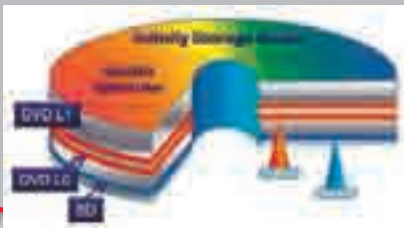
PARADOSSO DEI DIRITTI

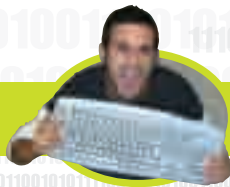
Il TG di Capodanno riportava che finalmente, dopo 70 anni di attesa dalla morte del loro creatore, i personaggi di Popeye (il nostro Braccio di Ferro) sono diventati patrimonio pubblico, almeno nell'ambito europeo. Allo stesso tempo viviamo in un sistema in cui i paradossi sui diritti d'autore si sprecano: se cediamo i diritti esclusivi di una nostra opera a un editore e questo, per la mancanza di entrate adeguate, decide di non distribuirla più, questa nostra opera rischia di morire del tutto senza che possiamo farci niente. E chissà quante volte è successo: autori emergenti che non raggiungono quote di mercato apprezzabili (leggi: soldoni per chi li pubblica) le cui opere finiscono dimenticate e inutilizzabili perché il detentore dei diritti non è più l'autore stesso. Ne vale la pena? La stessa Intel infatti sta sviluppando un driver open source che supporti le nuove specifiche da integrare nelle prossime release del kernel di Linux, che così per la prima volta sarà un passo avanti rispetto al sistema operativo di Microsoft. Non vediamo l'ora!

IN UE SMARTPHONE PIÙ CARI

L'Unione Europea ha proposto di innalzare la tassazione per i supercellulari, per gli smartphone insomma. Secondo la Commissione, i super telefonini dovrebbero essere ribattezzati "dispositivi multi funzionali" ed essere soggetti a una tassa appositamente istituita basata sulle dotazioni tecniche che presentano. Non c'è che dire, siamo d'accordo con Sony Ericsson: nel momento in cui tutti i produttori stanno tentando di contenere i costi e i prezzi al pubblico per incentivare i consumi, arrivano le autorità fresche fresche e impongono un balzello che inevitabilmente finirà per riflettersi sul prezzo finale dei prodotti. Siamo avvisati: se passa la regolamentazione, tutti i telefoni che saranno dotati di ricevitore TV, GPS, navigatori o Google Maps potrebbero costarci molto di più.

AL VIA IL BLU-RAY IBRIDO

Si tratta di un supporto che può essere riprodotto egualmente bene su un comune lettore DVD come su un moderno lettore Blu-ray, offrendo entrambi i contenuti. PonyCanyon, una sussidiaria di Fuji TV, è pronta a immettere sul mercato il primo prodotto commerciale su supporto multiformato contenente sia un DVD dual layer, riconoscibile dal laser di un comune lettore, sia un Blu-ray single layer, visto solamente dal laser di un adeguato lettore. Al prezzo di circa 300 € i consumatori giapponesi saranno i primi a sperimentare questa tecnologia, che però non vede niente di nuovo. Già da tempo, infatti, JVC prima e Toshiba poi avevano studiato supporti del genere, ma senza uscire dallo stadio di sperimentazione. Ora pare invece che la presenza sugli scaffali di questi supporti diventerà presto una realtà.

IL CELLULARE/AMBULATORIO

Alcuni ricercatori dell'università californiana UCLA sono riusciti a trasformare un comune telefono cellulare con fotocamera in un ambulatorio personale. Con un led ad alta luminosità, un filtro colorato e collegando il cellulare a un PC su cui gira un software scritto

POLIZIOTTO E RICATTATORE

Amerdeep Singh Johal era un poliziotto di Scotland Yard incaricato di mantenere il database della polizia denominato Crimint. Si tratta di un database contenente informazioni di vario genere, a cui la polizia in azione sul campo può accedere nel corso delle indagini. Questo l'uso normale; ma Amerdeep ha pensato bene di farci su la cresta, ricattando le persone i cui record sono presenti nel database e minacciandole di spifferare i loro segreti apertamente se non avessero pagato un riscatto. Le cifre richieste erano variabili, secondo la gravità dei fatti commessi dalle vittime, tra le 29 mila e le 31 mila sterline. In un caso sono state chieste addirittura 89 mila sterline. Ma chi doveva controllare sull'operato dell'agente? Se non fosse stato per un ricattato, che ha denunciato la cosa, Johal avrebbe potuto andare avanti ancora per anni.

R.I.P. MACWORLD EXPO

Gli addetti ai lavori e gli appassionati della mela morsicata di tutto il mondo se lo aspettavano, era nell'aria: Apple ha definitivamente rinunciato a partecipare all'organizzazione del Macworld Expo, ritenendo che i costi da affrontare e gli svantaggi della manifestazioni superano abbondantemente i vantaggi. Secondo indiscrezioni, la decisione sarebbe dovuta alle cagionevoli condizioni di salute del patron Steve Jobs, voci che già avevano provocato contraccolpi in borsa per il titolo Apple. Secondo Apple, invece, la partecipazione a una manifestazione del genere la costringerebbe ad avere sempre un nuovo prodotto da presentare, anche se immaturo e non pronto per il mercato, cosa contraria alla filosofia dell'azienda. Quanto sia vero dell'una o dell'altra versione non è dato saperlo, rimane solo la certezza che, molto probabilmente, Apple si sta avvicinando a un cambiamento epocale.

YOUTUBE SOTTO ACCUSA

Non tanto per il contenuto dei filmati che, cosa risaputa, spesso sono ai limiti della decenza e completamente inadatti agli utenti più piccoli. Ora si sta alzando un polverone anche sui commenti ai video postati dagli utenti: senza alcun controllo, contengono spesso parolacce, espressioni di sesso e violenza, link a siti pornografici e tante amenità simili. YouTube comunque si sta operando per migliorare il servizio anche sotto questo aspetto, ma ancora mancano controlli più approfonditi sui contenuti pubblicati, sui commenti e sulle immagini pubblicitarie. Siamo un po' alle solite: da una parte la libertà di espressione del popolo internettiano, dall'altra la necessità di crescere i propri figli protetti da materiali offensivi. A ogni modo, il controllo principale lo dovrebbero fare i genitori.

YouTube
Broadcast Yourself™

ad hoc, sono stati in grado di analizzare campioni di sangue e di rivelare la presenza di malattie come HIV o malaria e di compiere analisi sommarie sulla purezza delle acque. Secondo i tecnici responsabili dell'esperimento, il sistema non vuole essere un sostituto delle tecniche tradizionali compiute via microscopio, ma piuttosto un loro complemento, che aiuterebbe in situazioni di scarsità di mezzi. All'indirizzo http://newsroom.ucla.edu/portal/ucla/ucla-researchers-advance-lens-61847.aspx si trova la spiegazione tecnica dell'esperimento.

IN DIFESA DEL P2P

Mentre tutto il mondo rema contro e in Francia addirittura il presidente si interessa della questione, in Spagna un gruppo di manifestanti a favore del P2P è arrivata in piazza per difendere i diritti degli scaricatori internazionali. La manifestazione, annunciata con abbondante anticipo alle forze dell'ordine, ha avuto luogo a Madrid davanti all'ingresso del palazzo dove ha sede il partito al governo. I ragazzi manifestanti hanno compiuto operazioni di scaricamento pubblico di brani protetti da diritti d'autore, affermando poi che, dato che nessuno si è fatto vivo per arrestarli, scaricare audio, video e quant'altro dal Web è pienamente legale. Intanto la battaglia si sposta sul Web stesso, dove il sito della campagna governativa contro il P2P è alle prese con un sito identico ma contrario proposto da chi vuole smontare la tesi.

Fine della guerra tra le licenze del mondo "libero"

Open sì, ma quale licenza?

Da diversi anni, dal punto di vista della tutela delle opere, il mondo Open era diviso in due correnti distinte: quasi tutti i programmatori erano riuniti attorno alla Free Software Foundation mentre quasi tutti gli autori di materiale Open, musica, video, elementi grafici, usavano le licenze proposte dall'organizzazione Creative Commons.

La questione era tutt'altro che banale: entrambi i gruppi sostengono la libera circolazione delle idee ma da due prospettive differenti. La Free Software Foundation ha sempre avuto al centro del suo sistema di licenze il software e il materiale correlato, come Linux, mentre i Commoners, sostenitori della Cretive Commons, hanno sempre posto la questione sul piano dei contenuti, dedicando i loro sforzi a regolamentare la diffusione di musica, video, testi.

Le licenze Creative Commons hanno da sempre avuto la caratteristica di poter essere personalizzate nei dettagli, facendo scegliere agli autori se dare la possibilità di usare le opere in ambito commerciale o meno, di ammettere modifiche all'opera, di ammetterle attribuendo parte dell'opera finale all'autore originale o di impedirla, di cambiare la giurisdizione di validità della licenza in base alla nazione di appartenenza dell'autore e via dicendo. Le licenze FSF, invece, hanno da sempre avuto una maggiore rigidità, tipica dell'utilizzo in licenza del software. Due mondi separati in convivenza per diversi anni.

:: Insieme per forza

Alla fine, però, era destino che le due associazioni dovessero iniziare a confrontarsi e, in un certo senso, a scontrarsi. Se, per esempio, la FSF tutela il software e i manuali relativi, è ovvio che gli stessi manuali possano essere considerati anche normali opere che possono rientrare negli interessi principali delle licenze CreativeCommons. Allo stesso modo, un videogame non è solo un software ma ha sempre più punti in comune con un film e dispone di colonne sonore, elementi grafici e via di seguito.
Ulteriori problemi sorgono tutt'ora considerando le possibilità offerte all'utilizzatore del materiale, al fruitore. Come la possibilità di riutilizzare in parte o totalmente

Creative Commons, creativecommons.org, si è sempre distinta per l'attenzione verso le licenze dedicate a tutti i tipi di opera: dalla musica ai testi, dal software alla grafica.

GNU, www.gnu.org, ha dedicato la sua opera alle licenze per i software e, inevitabilmente, si è dovuta confrontare con le licenze Creative Commons dedicate alle altre opere.

l'opera originaria per creare qualcosa di nuovo, con la possibilità di riportare parti citando le fonti, con risultati diversi a seconda che si tratti di opere musicali o di opere letterarie o manuali e via dicendo.

La confusione, aumentata sempre più nel tempo, ha spesso costretto i creatori di contenuti, di qualsiasi tipo, a trasformarsi in legali per riuscire a identificare quale delle licenze disponibili facesse al caso suo. Senza contare, poi, le licenze prese originali trasformate nuovamente con clausole aggiuntive da parte di alcuni singoli autori, che hanno semplicemente aumentato il livello di frammentazione generale. Proprio questi si possono trovare, senza nemmeno rendersi conto, a infrangere licenze a causa di qualche dettaglio. Il problema delle licenze è così esploso in modo incontrollato negli ultimi anni.

Pensiamo, per esempio a un autore che desidera scrivere un saggio rilasciato sotto licenza Creative Commons in cui cita brani presi da Wikipedia, che usa una licenza FSF: le licenze risultano incompatibili e l'autore rischia di infrangerle entrambe. Lo stesso vale per un programmatore che vuole inserire un disegno rilasciato sotto licenza Creative Commons in un programma che usa parti sviluppate per Linux, rilasciato con licenza FSF. Una convivenza, quindi, che prima della grande svolta era molto difficile se non impossibile.

Queste considerazioni, unite alla naturale confluenza di tutti i generi di materiale, che sia audio, video, testi o software, ha aumentato sempre più il livello di confronto tra le associazioni e le licenze che propongono, destinandole a doversi assimilare e riconoscere a vicenda, a mettersi in contatto.

:: L'Open unito

Il primo passo l'ha fatto la Free Software Foundation che nella versione 1.3 della GNU Free Document License, meglio conosciuta come licenza FDL, ha aggiunto una sezione che consente ai wiki diffusi con quella licenza, come Wikipedia, di adottare anche la licenza Creative Commons Attribution Share-Alike versione 3.0. In pratica, la nuova licenza FDL permette di usare contemporaneamente la concorrente della Creative Commons. L'unico vincolo necessario è quello di usare la variante della Creative Commons che permette di riutilizzare l'opera commercialmente, attribuendone la paternità all'autore e consentendone ogni modifica. A dare risalto a questa notizia è il fatto che l'enciclopedia più diffusa al mondo, Wikipedia, è sempre stata distribuita con licenza FDL.

Una scelta fatta in origine dai programmatori che l'hanno fondata, perché era il tipo di licenza a cui qualsiasi programmatore faceva riferimento ma che rendeva incompatibili i termini d'uso di Wikipedia con quelli di moltissimi altri contenuti che facevano riferimento alle licenze CreativeCommons.
Un problema, quindi, che separava Wikipedia dal resto del mondo Open, impedendo una libera circolazione di contenuti che non rientravano nella licenza FSF e non potevano entrare in Wikipedia. Allo stesso tempo gli articoli che compongono Wikipedia non potevano essere riutilizzati in moltissimi altri contesti Open.

In attesa del rilascio della versione 2 della licenza GNU Free Document License, su cui si sta lavorando, questo aggiornamento alla versione 1.3 risolve i problemi creati da queste incompatibilità e apre uno spiraglio verso un mondo Open veramente unificato anche dal punto di vista legale.

È stato l'uso di Wikipedia, it.wikipedia.org, delle licenze GNU a dare i maggiori problemi di convivenza con le licenze Creative Commons e a dare inizio a un processo di unificazione che ancora non si è concluso.

INVISIBILITÀ TOTALE

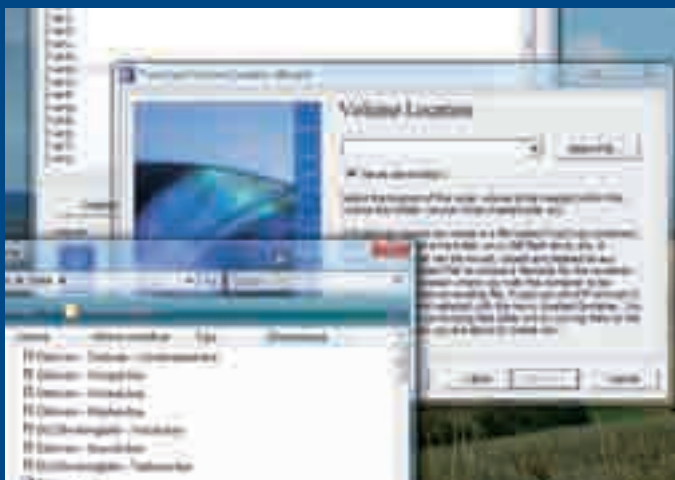
Rendiamo invisibili non solo i file ma anche le applicazioni

Per proteggere alcuni file dalla lettura da parte di persone non autorizzate, moltissimi si affidano ai sistemi di sicurezza offerti dai programmi. WinZip permette di indicare una password necessaria alla decompressione dei file, Word ed Excel hanno la possibilità di proteggere i file dall'apertura o dalla modifica e via dicendo. Purtroppo, però, questi sistemi di protezione sono tutt'altro che sicuri: anche se protetti, questi file hanno comunque caratteristiche che li rendono identificabili, sia nel nome che nella loro struttura interna. Così è possibile, usando programmi specializzati nell'analisi dei dati, trovare tutti i file di un certo tipo, anche se li abbiamo nascosti in qualche sotto directory e abbiamo avuto la cura di rinominarne l'estensione, rendendoli apparentemente inutilizzabili. Una volta identificato uno di questi basta applicare uno dei tanti programmi specializzati nella decifratura delle password per quel determinato tipo di file per ottenerne in breve tempo uno senza protezioni, spesso ricorrendo a semplici tecniche di brute force. La protezione offerta, quindi, è veramente scarsa e il recupero della chiave è solo una questione di tempo. Addirittura, moltissimi tipi di file non ammettono nemmeno questo livello di sicurezza: immagini, file di testo TXT o RTF, campioni audio Wav, file Mp3 e moltissimi altri tipi di file non dispongono di alcun livello di protezione.

:: Un file, un disco

La soluzione più pratica per risolvere questi problemi di sicurezza è quella di ricorrere a programmi di crittografia come TrueCrypt. Completamente gratuito, TrueCrypt si scarica dal sito www.truecrypt.org e permette di creare file che vengono usati come se fossero dei normali hard disk installati nel sistema. Dischi virtuali perché nella realtà sono, appunto, dei semplici file che possono avere il nome che desideriamo, possono essere nascosti in una qualsiasi directory dell'hard disk reale e, soprattutto, non hanno una struttura interna identificabile. In più, naturalmente, sono crittografati: per poterli usare devono essere decifrati e l'unico modo per farlo è quello di fornire al programma la password che abbiamo scelto quando li abbiamo creati. Grazie a queste caratteristiche è impossibile identificarli automaticamente e si rende necessaria un'approfondita analisi manuale per riuscire anche solo a trovare il file su cui poter tentare il recupero della password. Nel caso in cui si riesca a trovare il file corrispondente a un disco crittografato, però, possiamo comunque star sicuri che accedere ai file che contiene è tutt'altro che banale.

Tra le varie possibilità offerte da TrueCrypt c'è quella di poter combinare tra loro differenti sistemi di cifratura per ottenere un livello di sicurezza maggiore.

In fase di creazione di un disco crittografato, TrueCrypt ci permette di scegliere tra 4 differenti sistemi di cifratura selezionati tra i più sicuri al mondo. Come se non bastasse, questi 4 sistemi possono essere anche combinati tra loro, offrendo una garanzia assoluta di inviolabilità dei dati all'interno del disco. Rispetto ai sistemi di cifratura di singoli file, inoltre, TrueCrypt ha un vantaggio enorme: una volta fornita la chiave di decifratura al programma, il disco virtuale cifrato viene visto dal

Le directory di installazione dei giochi sono ideali per nascondere al loro interno i dischi cifrati con TrueCrypt.

La funzione di benchmark permette di controllare i tempi di lettura e scrittura dei dati usando metodi diversi di codifica.

sistema come un normale hard disk e può ospitare file di qualsiasi genere. Questo significa che possiamo installare un programma in un disco cifrato, vedere file video senza copiarli in altre locazioni, modificare i file con qualsiasi programma e senza nessun passaggio intermedio e via dicendo. Ovviamente, la sicurezza ha un costo: tanto maggiore è la complessità della cifratura e maggior tempo servirà per leggere e scrivere nel disco gestito dal programma, quindi non dovremo meravigliarci di avere tempi di salvataggio dei dati o di accesso decisamente più lunghi che con un disco reale.

Inoltre, come avviene per tutti i sistemi di cifratura sicuri, c'è il rischio concreto di perdere tutti i dati a causa della perdita della password: grazie alla possibilità di indicare password estremamente lunghe, cosa che il programma stesso consiglia, risulta praticamente impossibile ritrovare una password smarrita ricorrendo al brute force. Occorre fare un'attenzione particolare anche alla compressione dei file disponibile automaticamente con alcuni sistemi operativi come Windows Vista: per poter usare i dischi cifrati occorre disabilitare la compressione di sistema.

Un disco cifrato di TrueCrypt appare al sistema come un normale hard disk ed ha tutte le relative caratteristiche di flessibilità d'uso.

:: Qualche passo in più

La presenza del programma installato su un computer rappresenta un forte sospetto di presenza di dischi cifrati. Per evitare il problema possiamo copiare la cartella di installazione del programma su dispositivi rimuovibili come una chiave USB, rimuovendolo dal PC. Per chi desidera ottenere un livello di sicurezza in più, TrueCrypt mette a disposizione un sistema di cifratura speciale: un disco virtuale crittografato ospitato all'interno di un disco dello stesso tipo. Con questo sistema viene creato un disco crittografato normale in cui possiamo inserire alcuni file la cui sicurezza ci interessa poco. Nello spazio libero del disco crittografato viene creato un altro disco, con una password diversa e sistemi di cifratura differenti, che conterrà i dati che vogliamo realmente proteggere. In questo modo, anche nei casi in cui venisse trovato il disco cifrato e fossimo costretti a rivelarne la password, i dati da proteggere resterebbero nascosti: basterà rivelare la password del primo disco e non quella del secondo. Prima di ricorrere a questo livello di protezione, però, assicuriamoci di averne veramente bisogno: il tempo necessario per codificare e decodificare i dati può allungarsi di molto. Inoltre dovremo fare molta attenzione a non aggiungere dati al primo disco cifrato, quello con i file che ci interessano poco: diversamente scriveremo nella zona di quel disco usata per contenere i dati del secondo, rovinandolo irrimediabilmente.

Milano by sniff

Siamo andati in giro per le strade della città a caccia di reti wireless

Wireless è bello, comodo e... alla portata. Abbiamo già affrontato più volte il problema della sua sicurezza ma questa volta abbiamo voluto verificare "sul campo" la situazione e così abbiamo organizzato un piccolo ma significativo test nel cuore di Milano con un prezioso aiuto: piccolo, portatile e con su Linux. Si tratta dell'Acer AspireOne, un netbook versatile e facile da hackerare (HM 49). Dopo averlo studiato un po' lo si può adattare per compiere operazioni che non sono previste dal costruttore, come per esempio trasformarlo in una macchina per la caccia alle reti wireless. Ecco come abbiamo fatto.

:: Hacker Set

Il punto di partenza è l'Acer AspireOne con Linux preinstallato. In realtà si tratta di una versione Lite di Linus, una distribuzione orientale studiata appositamente per i sistemi embedded. Pur essendo abbastanza facile da modificare per i nostri scopi, in realtà si è trattato di un piccolo calvario: il software preinstallato è veramente ridotto all'osso e per aggiungere un qualsiasi programma bisogna prima perdersi nei meandri delle dipendenze. Anche se il sistema di ricerca delle dipendenze è automatico, non sempre le cose vanno come devono e non si trova una versione di un software adatta per funzionare su questa macchina. C'è voluto, insomma, un po' di tempo, prima di riuscire a far funzionare Aircrack-ng, la suite che abbiamo scelto per i nostri scopi. Stiamo parlando di una macchina in cui avremmo dovuto compilare del software ad hoc, ma che non ha installato né gcc né make!

Comunque, sul sito di Aircrack-ng sono elencati tutti i software che è necessario installare per il funzionamento della suite. La cosa più difficile da trovare e da far funzionare è il driver speciale per la scheda di rete: si tratta di un driver che permette la messa in modalità monitor della scheda, permettendogli di rice-

vere tutto il traffico wireless a portata di antenna. Per l'Acer AspireOne occorrono i driver Madwifi, ottimi ma disponibili sotto forma di sorgente da compilare e patchare con la patch fornita da Aircrack-ng. Questi driver sono quelli che hanno dato i maggiori problemi per la compilazione, dato che nel sistema mancavano molte librerie necessarie.
Trasformato l'AspireOne in una perfetta macchina per l'hacker, siamo partiti alla ricerca delle meraviglie metropolitane del wifi, non sapendo bene cosa aspettarci, ma ricevendo dopo tutto qualche bella sorpresa.

:: Ore 9 - Lambrate

La prima l'abbiamo avuta proprio qui, a due passi dall'ufficio. Accendendolo per iniziare una scansione, siamo riusciti a collegarci a una rete wireless completamente sprotetta che ci ha permesso di navigare sul Web! Ci aspettavamo di riuscire a entrare in qualche rete, ma non così facilmente. Normalmente però le cose non sono così semplici. Innanzitutto è bene sapere che cosa vogliamo cercare: reti wireless sì, tentare di connettersi sì, ma quali, e come?

Sappiamo bene che lo scoglio principale è scovare la password di rete, quella che viene usata come base per la comunicazione cifrata tra il client e l'access point. La sicurezza cifrata di una rete wifi può essere basata su tre tecnologie: WEP, WPA e WPA2, queste ultime due possono usare anche chiavi pre-shared (PSK). Una rete WPA/WPA2, a meno che chi l'ha installata non sia stato talmente poco furbo da usare una password facile da indovinare, è virtualmente impossibile da

Lo strumento dei nostri studi: un Acer AspireOne appositamente hackerato per poter eseguire programmi scelti da noi.

craccare (più che altro perché lo si può fare solo mediante brute forcing, e ci possono volere ere geologiche: provate il calcolatore all'indirizzo http://lastbit.com/pswcalc.asp). Aircrack-ng può craccare solo reti WPA/WPA2 che usano PSK, ma con tempi inaccettabili per i nostri scopi. Un altro discorso vale per le reti WEP: ne parleremo nel corso di questo articolo.

La prima zona che abbiamo monitorato, a parte la rete sprotetta di cui sopra, non ci ha dato molte soddisfazioni. Ci siamo resi conto poi che siamo in un periodo dell'anno poco favorevole: è appena passato Capodanno e molti sono in vacanza, e hanno spento le apparecchiature di casa. Poco male, ci accontenteremo di quello che è disponibile, siamo alla ricerca di reti WEP o comunque poco protette per vedere se l'Acer AspireOne può essere il nostro strumento perfetto. Risultato per Lambrate: una rete sprotetta e una WPA2, a distanza di poche centinaia di metri una dall'altra.

:: Ore 12 - Loreto

Ci aspettavamo che, avvicinandoci a zone più popolate di uffici e professionisti, avremmo trovato più materiale di studio.

Sul sito di Aircrack-ng sono presenti tutorial per apprendere le tecniche di base.

```
BSSID              PWR  Beacons   # Data  CH  MB  ENC  ESSID
00:A0:C5:9D:D5:5A  -54      281    29273  11  54  WEP  CrackMe
BSSID              STATION            PWR  Packets  ESSID
00:A0:C5:9D:D5:5A  00:90:4B:EB:9B:36  -53    13564  CrackMe
00:A0:C5:9D:D5:5A  00:17:3F:49:BB:07  -58    15772  CrackMe
```

Airodump-ng al lavoro su una rete di studio, durante la cattura dei pacchetti.

In realtà vale quanto detto poco fa: siamo in un periodo poco favorevole, pertanto non è stato facile trovare qualcosa da studiare. A nostro sfavore abbiamo anche il fatto che lavoriamo dalla strada, con un computer che, benché modificato nel software, non dispone di particolari strumenti hardware che ci consentano di potenziare i segnali ricevuti (non abbiamo antenne ultra potenti, non ci siamo costruiti una can-tenna con una chiavetta USB come hanno fatto molti hacker). I segnali che riceviamo sono quelli presumibilmente che giungono dai primi piani delle abitazioni, più vicino alla strada, e in effetti la loro potenza è stata sempre riportata nella fascia medio-bassa.

Nella zona di Loreto, all'angolo con viale Abruzzi, abbiamo scovato la prima rete WEP da studiare con il nostro piccolo mostro. Aircrack-ng, per craccare una rete WEP, necessita di un numero adeguato di pacchetti IV (Initialization Vector), pacchetti particolari che vengono trasmessi dall'access point wireless durante la procedura di collegamento con un client. Più sono e meglio è: il cracking di una password WEP si basa su dati statistici, quindi più ampia è la base di studio, più è facile scovare la password e avere accesso alla rete.

Purtroppo i vettori di inizializzazione non sono trasmessi spesso durante la normale comunicazione tra client e access point: in effetti servono per l'autenticazione all'inizio di una trasmissione e poi non vengono più usati. Possiamo agire in due modi: aspettiamo pazientemente di recuperare un discreto numero di pacchetti IV perché siamo abbastanza fortunati da trovare una rete con un buon traffico e diversi client collegati, oppure forziamo l'access point a ritrasmettere frequentemente pacchetti IV usando una tecnica di injection.
Per questo i driver della nostra scheda di rete sono "speciali", cioè modificati per poterla impostare in modalità monitor e per poter trasmettere pacchetti spurii che costringano l'access point a trasmettere i dati che ci servono. Oltre a questo, ci serve anche sapere il nome della rete wireless (SSID, per questo per proteggere la nostra rete di casa ci conviene disattivare la trasmissione dell'SSID una volta configurati i nostri PC per l'accesso alla rete) e su che canale trasmette l'access point. Sono dati che ricaviamo facilmente dalla scansione delle reti disponibili, perché ritrasmessi periodicamente da un access point impostato per il broadcast dell'SSID. Inoltre ci servono gli indirizzi MAC della nostra scheda di rete e dell'access point (quest'ultimo è trasmesso sempre nella solita trasmissione di broadcast).

La procedura da seguire con la suite di Aircrack-ng è la seguente. Innanzittutto, "spegnamo" i driver normali della scheda di rete con il comando airmon-ng stop ath0. Poi attiviamo i driver speciali con il comando airmon-ng start wifi0 n, dove n è il canale su cui trasmette l'access point vittima. Poi verifichiamo di essere nel raggio della portata dell'access point (anche se noi lo riceviamo, non è detto che siamo abbastanza vicini perché l'access point riceva le nostre trasmissioni): il comando è **aireplay-ng -n -e rete -a MAC-AP ath0**, dove n è il numero di canale, rete il nome della rete wireless e MAC-AP l'indirizzo MAC dell'access point. Tra i dati che otterremo in risposta è presente anche la bontà del segnale: più è vicina al 100% e meglio è, vuol dire che siamo a portata e possiamo trasmettere tranquillamente.

Ora iniziamo la cattura dei pacchetti IV, con il comando **airodump-ng -c n --bssid MAC-AP -w output ath0**, dove n è sempre il canale di trasmissione e MAC-AP l'indirizzo MAC dell'access point. Perché l'access point invii i pacchetti IV che ci servono dobbiamo essere associati con esso, altrimenti risponderà picche e scollegherà la trasmissione. Scriviamo quindi **aireplay-ng -1 0 -e rete -a MAC-AP -h MAC-PC ath0**, dove rete è il nome della rete wireless, MAC-AP l'indirizzo MAC dell'access point e MAC-PC l'indirizzo MAC della nostra scheda di rete. In questo modo l'access point ci associa come dispositivo accettato e ci invierà tutti i pacchetti IV di cui necessitiamo.
Solo quando saremo associati in maniera stabile, possiamo avviare la sessione di injection per fare in modo che l'access point ci ritrasmetta pacchetti IV fin quando necessario: aireplay-ng -3 -b MAC-AP -h MAC-PC ath0, valgono le regole dei comandi precedenti. A questo punto dobbiamo solo aspettare che uno dei client legittimi della rete tenti di comunicare con l'access point: aireplay-ng se ne accorgerà e inizierà a inviare richieste fasulle, e vedremo nella finestra di aerodump-ng il numero di pacchetti ricevuti aumentare velocemente.

```
12:14:06  Sending Authentication Request
12:14:06  Authentication successful
12:14:06  Sending Association Request
12:14:07  Association successful :-)
```

Aireplay-ng in funzione: dopo qualche tentativo siamo riusciti ad associarci con l'access point del malcapitato, per fortuna non abbiamo infierito.

Purtroppo in questo caso non siamo stati fortunati, non c'erano client in funzione e a noi ne serve almeno uno per poter ricavare la password di rete. Dopo diverso tempo e un paio di panini per pranzo, ci siamo diretti in un'altra zona della città.

:: Ore 16 - Niguarda

Anche in questo caso siamo stati abbastanza fortunati: dopo un primo momento di sconcerto, in cui non abbiamo ricevuto segnali della presenza di reti wireless, siamo riusciti a scovarne due raggiungibili dalla stessa posizione.

La prima e più forte era una rete WPA che abbiamo ignorato per focalizzarci sulla seconda, una nuova rete WEP. Qui siamo riusciti nel nostro intento: non divulghiamo naturalmente i dettagli della cosa, ricordiamoci che stiamo agendo a scopo didattico ma accedere a una rete wireless non di nostra proprietà è illegale e punibile dalla legge. Quello che possiamo dire è che, una volta ricevuti abbastanza pacchetti IV e lanciato il comando **aircrack-ng -z -b MAC-AP output*.cap** (MAC-AP sappiamo cosa significa, mentre output*.cap indica di usare tutti i file contenenti i pacchetti catturati da airodump) siamo riusciti a scovare la password di rete. Non abbiamo voluto infierire e non ci siamo collegati direttamente, ma abbiamo dimostrato che il wardriving con l'Acer AspireOne è possibile e può anche essere istruttivo e divertente.

:: Ore 20 - Navigli

Non ci siamo fermati al primo successo e abbiamo continuato il nostro

giro, spostandoci in zona Navigli per vedere se potevamo ripetere le operazioni descritte finora. Purtroppo niente reti WEP in questa zona, per lo meno nell'area in cui ci siamo fermati. Abbiamo voluto comunque provare a craccare una rete WPA2, non

Alla fine ci pensa Aircrack-ng a fare tutto il lavoro e a scovare la password della rete WEP.

ci siamo riusciti ma è stato comunque istruttivo. Per craccare una rete WPA2 (ricordiamoci che deve essere PSK altrimenti non c'è trippa per gatti...) abbiamo bisogno di catturare i quattro pacchetti di autenticazione di un client, indispensabili perché sono quelli in cui si cela la chiave PSK. Questo possiamo ottenerlo usando la tecnica di injection già vista per le reti WEP, oppure possiamo avere pazienza e attendere che un client si connetta alla rete. In entrambi i casi, quello che Aircrack-ng fa nel caso di una rete WPA2 è confrontare le parole contenute in un dizionario con i pacchetti di autenticazione ricevuti, per vedere se effettivamente una di queste parole è la chiave PSK. Va da sé che più è ampio il dizionario più avremo possibilità di successo, ma si tratta comunque di possibilità remote se chi ha installato la rete è stato abbastanza intelligente. In questo caso non abbiamo avuto fortuna.

:: Ore 23 - Corvetto

Prima di tornarcene a casa a riposare, dato che si è trattata di una giornata pesantuccia, abbiamo fatto un altro tentativo in zona Corvetto, purtroppo andato a vuoto. Non abbiamo trovato un'altra rete WEP da usare come materiale di studio e iniziavamo a essere troppo infreddoliti per ragionare lucidamente, e abbiamo deciso di mollare il colpo. Soddisfatti però, avevamo una teoria e l'abbiamo dimostrata.

La nostra macchina caccia WIFI si è dimostrata all'altezza della situazione e il livello di sicurezza delle reti wireless in città è decisamente più alto rispetto a quando queste reti hanno incominciato a diffondersi.

Privater

Segreti e sorveglianza a portata di clic sguinzagliando Google

GOOGLE INSECURITY

Rovistando sul Web possiamo trovare veramente di tutto, dalle informazioni utili per accrescere la nostra sete di conoscenza a quelle inutili come un innocente passatempo. Ma possiamo trovare anche (molto) facilmente l'accesso ad aree che, in teoria, dovrebbero rimanere riservate. Possiamo imbatterci fortuitamente in una di queste aree, oppure andare volutamente a cercarle. È il momento di scatenare tutta la potenza di Google.

:: Usiamo i parametri

Quando abbiamo bisogno di cercare qualcosa in Google, normalmente inseriamo qualche parola nella casellina di ricerca e facciamo clic su Cerca con Google. In base all'esattezza di quanto abbiamo inserito, possiamo essere abbastanza fortunati da trovare subito ciò che cerchiamo; in altri casi invece occorre andare un po' più a fondo, magari cambiando la stringa di ricerca. Se però vogliamo ottenere risultati certi, per quanto possibile, ci conviene imparare a usare i parametri che è possibile specificare attraverso la solita casellina di ricerca. Qui di seguito i "magnifici sei"; li conosciamo tutti ma è sempre bene rinfrescarsi la memoria:

- **"" (virgolette)**: tutto ciò che vi è contenuto deve essere considerato come un'unica espressione, pertanto vengono ritornati solo i risultati che la contengono esattamente.
- *** (asterisco)**: è il carattere jolly per eccellenza, quindi quando non ricordiamo come si scrive una parola o vogliamo allargare un po' i risultati contemplando forme plurali e singolari possiamo scrivere per esempio pecor* per ottenere sia "pecora" sia "pecore".
- **- (meno)**: esclude la parola che segue dai risultati; utile quando vogliamo eliminare un po' della fuffa che altrimenti ci verrebbe presentata cercando termini troppo generici (fa restringere il campo di ricerca).
- **filetype**: specificando un'estensione di file dopo i due punti, Google cercherà solamente le risorse di quel particolare formato (per esempio, cercando woodworking filetype:pdf troveremo solo documenti PDF che parlano di falegnameria).
- **inurl**: l'espressione che appare dopo i due punti deve apparire nell'indirizzo della risorsa individuata; immettendo per esempio arcuri filetype:jpg inurl:images troveremo solamente foto della nota soubrette.
- **intitle**: per i nostri scopi è uno dei parametri più interessanti e restringe i risultati solo alle pagine che mostrano l'espressione posta dopo i due punti nella barra del titolo.

Con Google possiamo trovare l'accesso, per esempio, a dispositivi come videocamere di sorveglianza.

:: Cosa cerchiamo?

Ci interessa arrivare proprio in quelle aree che dovrebbero rimanere riservate e che invece, per incuria o poca dimestichezza di chi le ha installate, sono state indicizzate e quindi rese disponibili a tutti. Stiamo parlando di videocamere di sorveglianza, stampanti online, cartelle non linkate direttamente a un sito e molto altro ancora. Se si sa bene cosa cercare, si può addirittura espandere la propria collezione di Mp3 o di film a spese di chi li ha "nascosti" sul proprio sito. Ovviamente sappiamo che non si può fare, non è legale, ma saperlo ci permetterà di non cascare negli stessi errori e di finire a fare le pecore...

:: Dispositivi hardware

Sul mercato sono sempre più numerosi i dispositivi informatici ed elettronici che dispongono di una connessione al Web. Per esempio, stanno prendendo molto piede le videocamere di sorveglianza che integrano un server Web accessibile mediante IP fisso, che permettono quindi di sorvegliare l'area coperta dal proprio PC di casa (o dal notebook se si è in viaggio). Il guaio è che se il software che le gestisce non è progettato a dovere (e di solito si parla di una qualche versione di Linux embedded, spesso messa insieme in fretta e furia senza adeguati test di sicurezza), queste risorse finiscono per essere indicizzate dai motori di ricerca e quindi potenzialmente accessibili anche da persone non autorizzate. Per trovarle dobbiamo conoscere che cosa appare nelle pagine di gestione del server Web integrato. Utili informazioni ci arrivano dai siti dei costruttori: qui spesso si trovano aree demo, in cui vengono proposte le immagini di videocamere piazzate su punti non strategici. Possiamo quindi scoprire che una videocamera è controllata da un particolare programma CGI, che si trova in una determinata cartella e che visualizza una pagina Web formata in una certa maniera. Per esempio, inserendo in Google la stringa **intitle:"INTELLINET" intitle:"IP Camera Homepage"** troveremo numerosi accessi a videocamere IP più o meno pubbliche.

Una stampante HP in linea. Non solo si può accedere al pannello di stato, ma si può anche stampare un documento.

Lo stesso succede per molti altri dispositivi: per esempio, durante le prove sono stati trovati numerosi siti per la stampa remota. Nel caso di un'università di Taiwan è stato possibile inviare in stampa un documento: non è dato sapere se poi la stampa ha avuto buon fine, dato che non ci troviamo fisicamente nella stessa stanza della stampante; tuttavia è segno che di porte aperte se ne possono trovare. Addirittura, in un caso è stato possibile accedere al pannello di configurazione della stampante, dove avremmo potuto cambiare l'IP sulla rete interna, i dati di accesso da amministratore o resettare la stampante.

Con i dati di login predefiniti si può accedere a queste cime di pini innevate mostrate da una videocamera di sorveglianza, ma potrebbe essere anche la targa della nostra auto...

:: Che pericoli si corrono

Non si tratta solo del pericolo che qualcuno violi la nostra privacy accedendo alle immagini di una videocamera di sorveglianza. Se non stiamo più che attenti, come nel caso della stampante citata prima, potremmo offrire facile accesso con diritti di amministrazione a malintenzionati che potrebbero sottrarci l'uso del dispositivo stesso. Finché si tratta di perdere qualche foglio di carta in stampe inutili può passare, ma se il dispositivo attaccato è il nostro router per la connessione a Internet?
Questi dispositivi hanno impostati di fabbrica i dati di login dell'amministratore (coppie login e password tipo admin/admin, pericolosissime). Basta scoprire di che dispositivo si tratta, visitare il sito del produttore per procurarsi il manuale (dove di solito sono citati login e password predefiniti) e tornare a farci visita. Cambiare i dati di login e aver cura che i file .htaccess e robots.txt nelle cartelle del server Web integrato contengano opportune indicazioni per evitare che il dispositivo sia accessibile ai motori di ricerca sono il minimo indispensabile per passare sonni più tranquilli.

Come assicurarsi che i file eliminati siano veramente irrecuperabili

CANCELLATO AL 100%

Quando cancelliamo un file, Windows non lo distrugge ma lo sposta nel suo cestino: una zona da cui è sempre possibile recuperare i file e usata per evitare errori di cancellazione.

Solo quando svuotiamo il cestino, il sistema provvede ad eliminare veramente i nostri dati. Questa operazione, però, avviene semplicemente eliminando dall'indice dei file presenti sul disco il file che era contenuto nel cestino: i dati all'interno del file restano fisicamente scritti sul disco e abbiamo l'impressione che non possano essere recuperati. Molti hacker ma anche esperti di sicurezza, usano spesso programmi facilmente reperibili come Sandisk RescuePRO, o PC Inspector File Recovery che possono ricostruire un indice sulla base dei dati realmente scritti sul disco, recuperando i file eliminati. Se l'eliminazione è stata un errore, siamo fortunati perché, a meno che qualche programma abbia sovrascritto i dati cancellati, potremo recuperare integralmente i nostri file.

:: Ancora presenti

Se vogliamo eliminare veramente i nostri file, però, l'esistenza di questi programmi può diventare un problema serio: basta pensare a cosa succede se buttiamo via un vecchio disco oppure se vogliamo eliminare la copia di un file che contiene le nostre password o altre informazioni che non vogliamo divulgare. Se il nostro computer cade nell e mani sbagliate rischiamo di non diffondere solo le informazioni che contiene ma persino quelle che ha contenuto in precedenza. Con gli strumenti giusti, basta qualche minuto e i file eliminati riappaiono quasi per magia e, con essi, i nostri dati, le nostre abitudini, i nostri segreti. L'unica speranza di evitare queste operazioni è che i file eliminati vengano sovrascritti da altri file ma si tratta di un'operazione casuale e in moltissimi casi è possibile recuperare anche solo qualche frammento di file che potrebbe contenere proprio le informazioni che desideriamo distruggere. In più, anche la sovrascrittura accidentale dei file non è una garanzia assoluta di aver definitiva-

La testina di un disco funziona in modo molto preciso ma ci sono strumenti che permettono di leggere i suoi errori e ricostruire i dati che sovrascrive.

La finestra principale del programma ha poche funzioni ma ci permette di indicare il sistema di sovrascrittura da usare per aumentare la nostra sicurezza.

Persino lo spostamento di un file può essere un problema per la nostra sicurezza ed Eraser ci permette di sovrascrivere automaticamente più volte la vecchia copia.

mente distrutto i file eliminati. Possiamo immaginare un disco fisso come se fosse diviso in milioni di quadrati di dimensioni microscopiche, che corrispondono alle possibili zone in cui la testina di lettura e scrittura si può collocare. Un file non è altro che una sequenza di 0 e 1 scritti all'interno di questi quadrati: una cifra ogni quadrato. Quando un file viene sovrascritto, la testina non fa altro che spostarsi in ognuna di queste posizioni e scrivere 0 o 1 a seconda del nuovo file, eliminando la cifra presente in precedenza. Se vivessimo in un mondo perfetto, quindi, un file sovrascritto sarebbe a tutti gli effetti irrecuperabile.

:: Il difetto che aiuta

Nella realtà, però, i componenti elettronici hanno alcune tolleranze, i motori che controllano le testine sono estremamente precisi ma non in modo assoluto, i magneti che scrivono i dati hanno una potenza che, anche se di pochissimo, può variare. Così, ogni scrittura in ognuno di questi quadrati può lasciare una specie di microscopica impronta della scrittura precedente: un po' come quando, in spiaggia, calpestiamo con il piede un'impronta precedente. È in questo modo che i difetti di scrittura su disco, del tutto trascurabili con il normale uso, possono diventare preziosi se si desidera recuperare questi dati sottoponendo il disco a un'analisi particolare, chiamata scansione elettronica della superficie. Questa operazione non fa altro che controllare ogni quadrato in cui è diviso il disco alla ricerca delle scritture imprecise e fornisce una specie di mappa dei dati scritti in precedenza. Il risultato di questa situazione è che nemmeno una formattazione completa del disco può garantirci che nessuno potrà mai recuperare i nostri file.

:: Scrivere e riscrivere

La soluzione a questo problema, senza nemmeno ricorrere alla formattazione, è quella di riscrivere più volte, con dati casuali, i file che eliminiamo. In questo modo, avremo la garanzia che anche l'analisi più accurata non potrà ricostruire alcun file perché confonderemo talmente tanto le impronte da rendere inservibile ogni traccia. Per farlo, però, occorre rivolgersi a programmi particolari, capaci di garantire che la scrittura avvenga ripetutamente e in zone precise del disco fisso: esattamente sopra i file che abbiamo eliminato. Il più diffuso programma di questo genere si chiama Eraser ed è attualmente utilizzato anche dalle forze dell'ordine e dai dipartimenti della difesa di molte nazioni, tra cui gli Stati Uniti. Completamente gratuito, si scarica dal sito http://sourceforge.net/projects/eraser e il suo funzionamento è quasi totalmente automatico. Una volta installato, si integra in Windows e aggiunge alcune voci al menu del cestino del sistema che ci permettono di svuotarlo sovrascrivendo i file con dati casuali. Il numero di sovrascritture varia a seconda delle nostre scelte e va dalla singola sovrascrittura con dati casuali, poco affidabile, fino ad arrivare alle 35 sovrascritture complete, in grado di rendere definitivamente impossibile qualsiasi recupero, anche con le tecniche più sofisticate disponibili nei migliori laboratori del mondo. Ovviamente, tanta sicurezza ha un costo: tanto maggiori saranno le sovrascritture e più tempo sarà necessario per portare a termine l'operazione. Ogni volta, però, potremo scegliere il procedimento più appropriato al tipo di file che desideriamo rendere irrecuperabili, magari usando poche sovrascritture per i file meno importanti e riservando un trattamento approfondito solo ai file riservati. Per essere sicuri che non si possano recuperare nemmeno i file temporanei, come molti dei file creati dal nostro browser, possiamo anche indicare al programma di non sovrascrivere solo i file che finiscono nel cestino ma anche quelli creati ed eliminati dai programmi: Eraser può essere configurato indicandogli scadenze in cui sovrascrivere tutto lo spazio libero del disco fisso in cui, probabilmente, sono contenuti i file eliminati.

L'integrazione di Eraser con il sistema ci permette di sovrascrivere più volte i file eliminati direttamente durante le operazioni fatte per svuotare il cestino.

Joomla Secure

Mettiamo in sicurezza il nostro sito Internet

Tra i diversi Content Management System (CMS) si sta affermando prepotentemente Joomla, un prodotto ancora relativamente giovane che permette però di gestire siti di qualunque dimensione data l'elevata scalabilità. Il team che lo ha sviluppato è nato da una costola della community di Mambo e in Joomla è stato ereditato in pieno il modello del prodotto open-source che permette di migliorare costantemente il progetto e che rende disponibile una quantità davvero enorme di plugin completamente gratuiti.
Come in ogni giovane progetto è necessario un certo rodaggio su strada, non solo del software in sé, ma anche del team che lo sviluppa e quest'estate è accaduto un fatto abbastanza increscioso (per altro assai frequente negli ambienti open-source): sono state infatti rilasciate delle patch di sicurezza, realizzate per chiudere una falla, senza informare i responsabili e chi aveva segnalato il problema, creando la falsa notizia che non fosse stata presa in considerazione, o fosse stato sottostimato il problema.
A seguito di questo incidente di percorso sono state estromesse alcune persone ed è stato ufficializzato il team dedicato alla sicurezza di Joomla: il Joomla Security Strike Team (JSST).

Foto di gruppo del JSST.

:: Il Joomla Strike Team

Il JSST si occuperà (e si sta già occupando) esclusivamente di gestire e migliorare la sicurezza del CMS. C'è una pagina ufficiale (developer.joomla.org/security.html) che spiega quali sono le linee guida adottate dal team, che non interviene solamente nelle situazioni critiche (come potrebbe essere la scoperta di una falla di sicurezza che affligge una particolare versione di Joomla), ma partecipa attivamente allo sviluppo del CMS per identificare e segnalare le potenziali debolezze del codice prima del rilascio pubblico dei sorgenti. Anche il logo (uno scudo stile medievale) non è niente male ed ha lo scopo di trasmettere

un messaggio chiaro: questi ragazzi sanno cosa vuol dire mettere in sicurezza un prodotto complesso come un CMS. Oltre a investigare e intervenire sulle vulnerabilità segnalate che affliggono direttamente Joomla e validare il codice prima del suo rilascio, il JSST aspira a divenire un punto di riferimento pubblico per ciò che riguarda la sicurezza e ad aiutare la comunità a comprendere l'importanza della sicurezza di Joomla. Il team è coordinato da Anthony Ferrara (che ricopriva già il ruolo di Core Team Member/Development Coordinator) ed è conosciuto sui forum di Joomla.org come "ircmaxell". Gli altri componenti della squadra sono persone che hanno avuto modo di collaborare con Joomla o sono esperti di sicurezza che sono stati arruolati per la prima volta nel progetto. Tra di loro è presente anche un italiano, Emanuele Gentili, che ha parlato probabilmente per primo di una vulnerabilità scoperta in Joomla pochi giorni prima dell'annuncio della nascita del team.

Anthony Ferrara ha dichiarato che la squadra appena nata stava già lavorando per identificare ogni problema riscontrato da Joomla 1.5.0 in avanti (l'ultima versione rilasciata è la 1.5.8) attraverso un'approfondita analisi del codice. Nel frattempo, il sito del JSST viene utilizzato per pubblicare tutti i problemi rilevati in Joomla e gli articoli relativi alla sicurezza pubblicati dal team (è presente un feed e ci si può abbonare direttamente online per essere sempre aggiornati).

A seguito delle incomprensioni passate, è stata anche codificata una policy relativa al comportamento da adottare nel caso venisse rilevata una falla di sicurezza: le vulnerabilità verranno rese note solamente dopo che è stata realizzata e rilasciata un release che risolve il problema i bollettini di sicurezza (advisory) saranno dettagliati a sufficienza, ma non così tanto da permettere a chiunque di realizzare attacchi in grado di bucare un sito senza alcuna difficoltà (come è già accaduto).

I PRINCIPALI CMS

Tra i CMS principali, oltre Joomla ricordiamo:

- **Mambo: il progetto iniziale da cui è nato per scissione Joomla; il progetto è maturo e il software permette un elevato grado di personalizzazione. Caratteristici i MamBot: componenti software che possono essere lanciate anche in background e svolgono dei compiti prestabiliti.**
- **OpenCms: la caratteristica peculiare di questo prodotto è quella di essere basato su Java e XML**
- **PHP-Fusion: questo CMS è ampiamente utilizzato anche da siti italiani, famoso per la semplicità di gestione**
- **WordPress: orientato ai blog, permette di sollevare l'autore da tutte le problematiche inerenti la gestione del sito web e del database; i numerosissimi plugin sono semplicissimi da installare e da aggiornare (anche automatico).**

Il JSST dovrà di conseguenza monitorare anche gli articoli su Joomla pubblicati in rete per verificare sia che le informazioni riportate siano corrette (e non manipolate), sia per richiedere l'oscuramento di pagine web relative a falle di sicurezza fintanto che non siano disponibili contromisure (in riferimento alla policy). Questa politica è certamente opinabile, ma è comprensibile che si voglia chiedere un comportamento corretto nell'ambiente tipicamente anarchico della rete. È chiaro che poi ognuno è libero di comunicare come meglio crede le informazioni di cui dispone, in internet.
Sempre sul sito del JSST è disponibile anche un form (all'indirizzo developer.joomla.org/security/contact-the-team.html) da utilizzare per riportare una eventuale nuova vulnerabilità. Fa sorridere, ma chiunque segnalerà una falla effettivamente presente, riceverà in regalo una T-shirt di Joomla!

:: Quali vulnerabilità ci sono

L'ultima vulnerabilità pubblicata è del 10 novembre scorso ed ha di fatto coinciso con il rilascio dell'ultima versione di Joomla (1.5.8) dal momento che affligge tutte le versioni di Joomla (la serie 1.5.x e precedenti). La falla, ad impatto classificato come moderato, è stata recepita il 9 novembre e il giorno dopo era disponibile online la nuova release di Joomla con relativo advisory

Alcuni suggerimenti sulla sicurezza del proprio CMS proposti dal JSST.

Per essere più al sicuro conviene aggiornare Joomla all'ultima versione disponibile.

che illustrava un problema relativo alla possibilità di inserire codice malevolo nel titolo e nella descrizione di post di weblink, sia lato amministratore che semplice utente, tramite il modulo com_weblinks. Per la chiusura della falla è necessario obbligatoriamente effettuare l'upgrade alla versione 1.5.8.
Altre falle possono coinvolgere i singoli plugin, tuttavia molte vulnerabilità dipendono anche dall'utilizzo "non sicuro" del codice che si può inserire in un sito web che utilizza Joomla. È il caso, abbastanza diffuso, relativo al parsing SQL pivo di alcuni controlli mirati ad evitare SQL Injections. Lo stesso Anthony Ferrara ha scritto un articolo apposito in cui analizza la problematica e indica come scrivere codice sicuro (vedi "Preventing SQL Injections" nel sito di Joomla).

:: Come chiudere le falle

In generale non vengono rese disponibili le patch individualmente e si deve procedere ad aggiornare completamente l'installazione di Joomla. Personalmente ho speso del tempo per effettuare l'upgrade su Wordpress all'ultima versione e nonostante avessi fatto un backup del database e uno dell'interfaccia, ho incrociato le dita finché non ho visto ricomparire online tutto funzionante. Con Joomla, al contrario, viene reso disponibile oltre al pacchetto standard ("stable") per le nuove installazioni, anche il pacchetto "upgrade" che permette una migrazione semplificata verso la release più nuova.
Viene comunque consigliato di effettuare prima un backup e verificare il corretto aggiornamento su un sito di test quanto più possibile gemello del sito da aggiornare, prima di procedere. Se comunque qualcosa dovesse andare storto, anche seguendo le informazioni ufficiali (docs.joomla.org/Upgrade_Instructions), si può comunque contare sul forum (forum.joomla.org) al quale partecipano utenti molto competenti sparsi in tutto il mondo (e quindi c'è sempre qualcuno online in grado di darci un feedback, se proprio non troviamo l'argomento già trattato in qualche post).
Diverso discorso per i plugin che solitamente possono essere aggiornati in modo indolore: sia che l'aggiornamento venga svolto da interfaccia amministratore, sia che venga effettuato l'upload (via FTP), si tratta di sostituire alcuni file di servizio che non impattano necessariamente con il contenuto del sito. In questo caso il backup si risolve nel copiare offline la cartella da aggiornare e se c'è qualche problema è facile tornare indietro.

Massimiliano Brasile

HACKER MAGAZINE 49

Troviamo il tutorial sull'installazione di Joomla nel numero 49 di Hackers Magazine in edicola a gennaio 2009.

CREA IL TUO SITO DI
HACKER JOURNAL

Come i cracker usano i loro strumenti per rubarci l'account di Windows Live Messenger

MSN HACK

Windows Live Messenger, l'attuale versione di MSN Messenger, è un po' come il televisore, ormai è in tutte le case. È un modo semplice e immediato per farsi nuovi amici e tenersi in contatto con quelli vecchi, e nelle ultime versioni dispone di strumenti utili e divertenti per compiere molte azioni. Come ogni software di comunicazione, però, deve essere usato con un po' di sale in zucca.

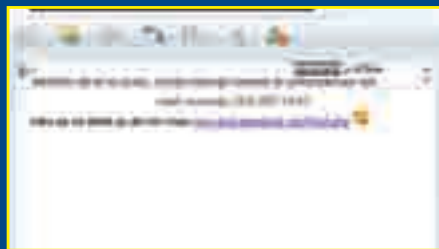
:: L'uso normale

In realtà, Windows Live Messenger funziona benissimo già così come lo si trova. Ma è nella natura hacker tentare di alzare il cofano e vedere cosa c'è sotto, e magari cambiare lo stato delle cose, ognuno secondo le proprie possibilità. Il minimo che si possa fare è quindi installare Messenger Plus! Live, un add-on che da solo permette di cambiare molte cose del funzionamento del messenger. Nella maggior parte dei casi si tratta di cambiamenti estetici: aspetto delle finestre, possibilità di personalizzazione grafica con le skin, uso di colori e stili diversi nel testo e così via. Altre funzioni utili comprendono il raggruppamento delle chat in un'unica finestra divisa in schede, funzioni avanzate per la gestione della lista dei contatti e la possibilità di espandere il programma per mezzo di script. Le possibilità, quindi, sono virtualmente infinite, ma questo è alla portata di tutti.

:: Crackers e MSN

Data la sua enorme diffusione, è facile intuire che questo messenger è uno strumento utile non solo per gli utenti normali, ma anche per chi vuole farsi i fatti degli altri. È ormai diventata una piaga il diffusissimo MSN Virus: un messaggio inviato da un cracker che finge di

All'indirizzo http://www.msgpluslive.it/scripts/browse/ troviamo una fornita collezione di script per Plus!

essere uno dei nostri contatti che invita a scaricare una foto o a visitare un sito (la foto, chissà perché, è un eseguibile compresso in un file ZIP che non viene nemmeno rilevato dagli antivirus, già questo comunque dovrebbe insospettirci). In entrambi i casi viene eseguito un programma sul PC della vittima che invia al cracker login e password di MSN, oltre a inviare lo stesso messaggio della foto a tutti i contatti presenti nel proprio elenco. Tristemente famoso perché, quando a essere infettato è un nostro amico, i messaggi di invito a scaricare il virus truccato da foto sono talmente assillanti da essere tentati a bloccarlo finché non risolve il problema.
Per aiutarlo possiamo invitarlo a cercare con Google e a usare il programma MSNFix, in grado di scovare e rimuovere definitivamente il virus.

Il noiosissimo virus per MSN, in questo caso rimanda la vittima su un sito Web ma esiste anche la versione "locale" che fa scaricare un file infetto.

Un tempo (sono stati rimossi per non ben definite questioni), giravano su YouTube video di cracker in azione con questo virus: un programma appositamente scritto crea un eseguibile contenente il virus non rilevabile dagli antivirus comuni e lo zippa in un file, il quale viene inviato al contatto vittima. Il più è convincere la vittima, con un po' di social engineering, a eseguire il programma, ma superato questo scoglio si avrà il controllo completo del suo account MSN, che potrà quindi essere usato per inviare il virus a N altre persone aspettando che si infettino. Lasciando aperto il programma sul suo PC, il cracker riceve automaticamente, non appena una vittima si connette, un messaggio contenente login e password dell'account MSN che usa, e qui il cerchio si chiude (in pratica si può andare avanti all'infinito, fintanto che sempliciotti del Web cascano nel tranello).

:: Webcam hacking

Con un procedimento simile si può addirittura prendere il controllo della webcam del contatto vittima. La chiave ancora una volta sta in un file che deve essere eseguito dalla persona presa di mira. In questo caso però non gli ruba l'account, ma installa un miniserver che invia l'immagine ripresa dalla sua webcam a un programma client in funzione sul PC del cracker.

Questo video su YouTube mostra la procedura e i programmi da usare per rubare il video trasmesso dalla webcam del contatto vittima.

La cosa più difficile, se così si può dire, è scovare l'IP della vittima: a questo scopo si possono usare appositi script per il pacchetto Plus! di cui abbiamo parlato in precedenza, o usare il comando netstat /n dal prompt dei comandi di XP e spulciare gli IP indicati fino a trovare quello giusto. Esiste anche un programma che permette di scovare l'IP semplicemente portando la sua finestra sopra quella della conversazione con il contatto, ma naturalmente non si tratta di un software affidabile data la provenienza (viene segnalato come pericoloso anche dagli antivirus). Una volta ottenuto l'IP dell'ignara vittima, lo si dà in pasto al programma client et voilà, avremo in una finestra a parte il video catturato dalla webcam. L'unico dubbio che rimane, e che i forum sul Web non hanno chiarito, è come si comporta la spia di accensione della webcam stessa: non pare possibile che possa rimanere spenta, ma probabilmente il cracker si assicura a priori che il contatto vittima già stia usando la webcam per "nascondere" la propria attività spionistica.

:: Elenco contatti

Numerosi siti promettono di scovare chi ci ha eliminati o bloccati dal proprio elenco contatti. Inutile rimarcare il fatto che si tratta di promesse da marinaio: in alcuni casi è solo un modo per appropriarsi del nostro indirizzo o peggio del nostro intero account. Mentre non esiste alcun modo per sapere chi effettivamente ci ha bloccati, esiste un sistema (ma non è infallibile) per sapere chi ci ha eliminati dalla sua lista: apriamo la finestra delle opzioni (Strumenti/Opzioni) e attiviamo la scheda Privacy.

Un sistema per verificare se siamo stati eliminati da uno dei nostri contatti.

Facendo clic destro su ogni contatto presente nel riquadro Elenco Consenti e verificando lo stato del comando Elimina, se lo troviamo in grigio e inattivabile siamo ancora nella lista di quel contatto, se invece è nero e selezionabile ci ha probabilmente eliminato. Nel Plus! questo strumento è presente sotto forma di apposita funzione (menu Plus!/Pulizia lista Contatti). Se non vogliamo invece permettere a un nostro amico di bloccarci, all'indirizzo http://software-world.forumcommunity.net/?t=11008416 troviamo un trucco per il Plus! sotto forma di script.

"HOME": BUG PERICOLOSI

Esce il social network in 3D per la console di Sony, tra luci e ombre: le seconde, però, sul versante sicurezza, superano le prime

Dopo tanta attesa, anteprime, voci di corridoio e mesi di sviluppo, ecco Playstation Home. Di cosa si tratta? Di un social network del tutto riconducibile a Second Life, quindi un vero e proprio mondo virtuale nel quale i videogiocatori si incontrano, scambiano qualche battuta, fanno amicizia, organizzano partite e, nei prossimi progetti di Sony, faranno acquisti online. Insomma, c'è parecchia carne al fuoco, specie se si considera che tutte queste forme d'interazione poggiano su una struttura network complessa, e arricchita da un comparto grafico 3D che, sulla carta, sfrutta le potenzialità dell'elegante architettura hardware di PS3. Già, "sulla carta", perché in realtà sul servizio si sono sollevate parecchie critiche, buona parte delle quali rivolte proprio a una fattura tecnica non certo di prim'ordine. I numerosi aggiornamenti, per fortuna, hanno sistemato parecchie magagne, ma molto deve ancora essere fatto.

:: Qualche errore di troppo

Anzi, a dirla tutta, uno dei principali problemi, nel momento in cui scriviamo, serpeggia ancora tra le righe di codice di Home.

Rispetto alla precedente versione, Playstation 3 integra il pieno supporto alla Rete. Ma ci vuole software di qualità.

E non si tratta di quisquilie: è ormai assodato, infatti, che lo sviluppo di Home abbia preso alla leggera alcuni aspetti legati a doppio filo alla sicurezza informatica. Visto che in ballo, dopotutto, ci sono dati personali di milioni di utenti, non è certo cosa da poco.
Ma andiamo con ordine. Le cronache narrano che il progetto Home derivi in realtà dal videogioco "The Getaway Online", versione multiplayer di un titolo che, a fronte di costi di sviluppo da produzione hollywoodiana, si rivelò un mezzo fiasco in fatto di vendite.
Al punto che, proprio il progetto "Online", la cui lavorazione iniziò prima della commercializzazione del titolo originario, fu poi fermato.

Buona parte della struttura di "Home" deriva da "The Getaway Online".

Qualche tempo dopo, Phil Harrison, approdato da poco a Sony come presidente di Sony Computer Entertainment Worldwide Studio (in pratica il "capoccia" del reparto ricerca & sviluppo), sponsorizzò l'idea di un mondo virtuale con cui rafforzare la community degli utenti PS3.
E visto che una struttura tecnologica, in fondo, era già pronta, perché non utilizzare quella? Detto e fatto, dalle ceneri di "The Getaway Online" ecco nascere Home. Peccato che gli sforzi per aggiornare il progetto siano andati in buona parte alla "carrozzeria", vale a dire grafica e sonoro, mentre l'impressione è che il cuore, cioè le funzioni online, siano state mutuate un po' troppo pesantemente dal titolo videoludico. Che era per Playstation 2, e fu progettato in un periodo (circa il 2003) in cui le tecnologie Internet erano decisamente più antiquate.

:: Su grafica e sicurezza

E così eccoci ai giorni nostri. Home, dopo una fase di collaudo interno, è ufficialmente lanciato in versione e, dopo appena qualche giorno, e anche alla luce dei succitati aggiornamenti, saltano fuori le grane più evidenti.
Come quelle grafiche rivelate dai video su http://www.youtube.com/watch?v=0DWIcSuJ8TE e su http://www.youtube.com/watch?v=_UPMnFFoIt4&NR=1. O come quella legata squisitamente legata alla sicurezza. È emerso, infatti, che la connessione tra ciascuna console e i server di Sony che gestiscono Home non sia protetta. In alcun modo. Non è uno scherzo, purtroppo: nessun tipo di crittografia è pronta a codificare i dati ricevuti e inviati da e verso i server, rendendo applicabili anche le tecniche di sniffing più elementari. Sony risolve subito il problema? Macché: si occupa, piuttosto, di far oscurare tutti i siti che ne parlano, lasciando il baco e palesando una vulnerabilità che fa temere il peggio per i poveri utenti.

:: Nozioni di base

Già, perché basta avere delle modeste conoscenze di hacking per riuscire a combinarne di tutti i colori nei server Sony, anche se, pare, le modifiche apportate sono fruibili solo dalla console da cui sono apportate.
Si arriva così al caso estremo di un utente del sito PS3Hax.net, che proclama di essere riuscito a cambiare alcuni dei poster che adornano il mondo virtuale di Sony. La tecnica è elementare: dopo aver installato Apache HTTP Server, scaricabile da (http://rapidshare.com/files/173698264/apache_2.2.10-win32-x86-openssl-0.9.8i.msi), e Simple DNS Plus (basta la versione "trial"), scaricabile

Simple DNS Plus mette KO il sistema di (non) sicurezza di Home.

da http://rapidshare.com/files/173697154/sdnsplus-setup.exe; andiamo alla sottocartella /Program files/Apache Software Foundation/Apache 2.2/htdocs. Estraiamo qui i file dell'archivio scaricabile da http://bluehost.to/dl=7qjYfKcaL. Fatto questo, avviamo Simple DNS Plus. Clicchiamo su Records e su Quick.
In Zone Name scriviamo scee-home.playstation.net, mentre in Web server IP il nostro indirizzo IP.
A questo punto, dal menu dalla PS3 andiamo nella sezione Network, impostiamo su "manuale" il DNS server e inseriamo anche qui l'indirizzo IP. Andiamo quindi in htdocs, su c.home\prod\live\Screens. Sorpresa: qui troviamo il file CinemaChannels.xml. Aprendolo, troviamo il nome dei file video che sono mostrati nel cinema (in formato mov, ma sono supportati anche gli mp4). Basta modificare il nome dei file e l'hack è bello che fatto. L'unica accortezza finale è quella di riavviare Home, per rendere effettive le modifiche.

Nuova vita al laser

Costruiamo un potente raggio laser recuperando un vecchio masterizzatore dvd

Tutti o quasi abbiamo in casa un vecchio masterizzatore dvd non funzionante o comunque obsoleto in attesa di terminare la propria carriera in una discarica. Esiste un modo per evitargli, o almeno a qualche suo componente, una fine così ingloriosa: con un po' di pazienza e con le istruzioni che seguono, possiamo estrarre il diodo laser per costruire una potente torcia laser, un apparecchietto molto simile, in apparenza, ai classici puntatori che troviamo in vendita per pochi euro ma decisamente molto più potente. Niente di estremamente futuristico, certo, ma il divertimento non sta nell'obbiettivo finale quanto nel raggiungerlo. E allora mettiamoci all'opera.

:: Le raccomandazioni

Prima di iniziare vogliamo ricordare che l'oggetto che si ottiene non è un giocattolo, ma un laser in grado di danneggiare permanentemente gli occhi o di causare ustioni. Inutile sottolineare che non ci assumiamo alcuna responsabilità per un suo eventuale uso improprio...

:: La lista della spesa

Ovviamente serve un masterizzatore. Un 16x è l'ideale; in alternativa è possibile acquistare il solo diodo da qualche negozio di elettronica oppure su eBay, per 15-20 euro (ma dove va a finire il divertimento?). Poi serve un contenitore nel quale assemblare il tutto; si può utilizzare uno di quei puntatori laser di cui si parlava unito a una mini torcia possibilmente di metallo. In questo caso avremo anche a disposizione la lente per mettere a fuoco, altrimenti dovremo procurarcene una e adattarla. La possiamo trovare in una vecchia webcam, oppure in una fotocopiatrice laser rotta, in discarica.
La lente è necessaria per la corretta focalizzazione del raggio; usandone una da puntatore, è probabile che la convergenza avvenga tra i 30 e 150 cm. Il massimo sarebbe poter disporre di una ghiera filettata per cambiare punto di messa a fuoco. Se vogliamo essere sicuri di non distruggere il diodo, sarebbe molto utile prevedere anche un piccolo circuito driver per la regolazione della tensione, per evitare inutili arrabbiature derivanti dalla cottura dei diodi.

Gian Franco Baroni

IL REGOLATORE DI TENSIONE

Per i più tecnici, ecco un semplice schema di regolatore di tensione. La tensione va misurata ai capi 1 e 2 dove andrebbe collegato il diodo, a valle della resistenza da un ohm. Il circuito è molto semplice e poco costoso; un peccato non costruirlo.

SMONTAGGIO DEL MASTERIZZATORE

Una volta smontato il masterizzatore, localizziamo il diodo: normalmente in un masterizzatore sono presenti due laser, quello di lettura e quello di scrittura. Per i nostri scopi, occorre prelevare ovviamente quello incaricato di scrivere il supporto. Di solito emette sul rosso e ha solo 3 pin saldati sulla piastrina che lo tiene ancorato alla staffa precedentemente rimossa. Con molta cautela, dissaldare il componente.

SMONTAGGIO DEL MASTERIZZATORE

Per essere sicuri di aver rimosso il diodo corretto, è possibile collegare ai pin una tensione proveniente da due batterie stilo da 1,5V. Se il diodo si illumina, tutto ok. La figura mostra il diodo dal lato inferiore.

SMONTAGGIO DEL MASTERIZZATORE

Occorre saldare (sempre con estrema cura) due spezzoni di filo ai poli negativo e positivo come illustrato nello schema.

SMONTAGGIO DEL MASTERIZZATORE

Ecco come appare il diodo, una volta estratto.

MODIFICA DEL PUNTATORE LASER

Ora occorre smontare il puntatore laser acquistato con pochi euro per per sostituire il diodo a bassa potenza con quello estratto dal masterizzatore.

MODIFICA DEL PUNTATORE LASER

Una volta aperto il puntatore, procedere alla sostituzione del diodo:

INSTALLARE NELLA TORCIA

Siamo quasi alla fine; ora occorre disassemblare la torcia e montare il puntatore modificato.
Molto importante è allargare il foro del riflettore fino a raggiungere la misura adatta.

INSTALLARE NELLA TORCIA

Quindi montiamo il puntatore al posto della lampadina.
La lente in plastica della torcia va rimossa; inseriamo le batterie nella torcia (previo controllo della polarità) e il gioco è fatto...

INSTALLARE NELLA TORCIA

GOOGLE PHONE: L'HACK PERFETTO

A poche settimane dall'uscita del "G1", molti hacker si sono sbizzarriti, scovandone funzioni e procedure da leccarsi i baffi

Sul T-Mobile G1, detto anche "Google Phone", aleggia una certa confusione. Che parte proprio dal suo nome: quello corretto è il primo, mentre il secondo non rende dovuta giustizia al fatto che il telefono NON è stato sviluppato da Google, ma proprio da High Tech Computer corporation. Google, invece, ha sviluppato il software che anima il dispositivo, vale a dire il tanto strombazzato Android. È il sistema operativo mobile delle meraviglie: basato su Linux (wow!), è completamente aperto e adattabile ai più svariati dispositivi portatili. La versione installata nel G1, quella del debutto, ha peccato un po' in presunzione, mostrando numerosi bug che, per fortuna, aggiornamento dopo aggiornamento, sono diminuiti in numero e gravità. Sebbene sia difficile stabilire delle procedure di hacking che funzionino su qualunque G1 (dipendono molto dalla versione installata), noi ci proviamo, descrivendone due che stanno facendo parlare molto di sé.

::Installare le applicazioni

Innanzitutto, vediamo come installare applicazioni di terze parti sul telefono di HTC. È noto infatti che benché Android sia un sistema operativo aperto, l'aggiunta di software esterno è alla mercé dei soli sviluppatori. E di quanti hanno per le mani l'SDK (Software Development Kit), cioè l'ambiente di sviluppo.
Il primo passo, infatti, è scaricare l'SDK, che troviamo all'indirizzo code.google.com/android/intro/installing.html. Una volta scaricato l'archivio zip che lo contiene, estraiamone il contenuto annotando le cartelle di destinazione. Cerchiamo di mantenere quelle predefinite, in particolare le sotto-cartelle tools e samples.
Se utilizziamo Windows, a questo punto selezioniamo Start/Computer e, da questa finestra, clicchiamo in alto, su Proprietà del sistema. A sinistra clicchiamo su Impostazioni di sistema avanzate.

Poi, clicchiamo su Variabili d'ambiente. Nella sezione Variabili di sistema, scorriamo l'elenco e facciamo doppio clic su Path.

In questo articolo parliamo dell'utilizzo dell'SDK in Windows, ma l'apposito sito elenca anche le procedure per Mac e Linux.

Alla fine della stringa Valore variabile aggiungiamo infine tools/. Clicchiamo su OK in tutte le finestre, per chiuderle.
Una volta che l'SDK è installato, scarichiamo (ma non installiamoli ancora) i driver che consentono di collegare il G1 alla porta USB del computer.
Li troviamo direttamente su http://dl.google.com/android/android_usb_windows.zip.

Fatto questo, passiamo al nostro amato G1: dal menu selezioniamo Settings e quindi Application settings, e attiviamo Unkwown sources. Poi, sempre da Settings, selezioniamo Application settings e quindi Development. Da questa schermata attiviamo la voce USB debugging.
Solo dopo aver fatto questo, colleghiamo il telefono al computer, tramite un cavetto USB. Quindi, installiamo i driver che abbiamo precedentemente scaricato.
Di fatto, ora è tutto pronto per poter installare una qualsiasi applicazione nel nostro G1. Il telefono di HTC è riconosciuto da Windows come "ADB Interface", o un nome similare.
Le applicazioni per Android sono in formato APK, e per installarle basta copiare il file desiderato in una cartella del disco fisso. Quindi, direttamente dal telefonino, impartiamo un comando del tipo adb install c:\cartella, dove per c:\cartella c'è il percorso e la cartella dove è presente il file APK.

::Il "famoso" bug

Il G1 è salito agli onori della cronaca hacking per aver palesato uno dei più grossolani bug degli ultimi tempi. Un bug attivo fino al firmware in versione RC29, mentre le successive, per fortuna, lo hanno corretto. Per sapere quale versione troneggia nel nostro telefono, dal menu principale selezioniamo Menu/Settings/About phone.

Osserviamo poi la stringa che segue Build number. Se termina con RC29, o inferiore, allora il dispositivo è ancora "sensibile" al bug. Già, ma come funziona?
In pratica, tramite la tastiera, basta seguire le seguenti istruzioni:

premere **RETURN**

digitare **REBOOT**

premere di nuovo **RETURN**

Il telefono, come per magia, interpreta la stringa come un comando di sistema, riavviando il software del dispositivo. Questo è solo un esempio delle conseguenze devastanti che un bug di questo tipo può avere. Per i più smaliziati, è anche interessante conoscer eil motivo che sta alla base di questo errore nel software del G1. SI tratta di poche righe di codice contenute in /init.rc. E precisamente:

```
## Daemon processes to be run by init.
##
service console /system/bin/sh
   console
```

Visto? Quattro righe di codice lasciate per sbaglio tengono attiva una console che intercetta i testi scritti come comandi (posto che I testi corrispondano effettivamente a dei comandi!).

Al comando reboot visto poco fa, si aggiunge così, per esempio, anche cat. Questo disabilita la shell, disattivando dunque il bug fino al riavvio successivo della macchina . Un mezzo efficace per limitare eventuali danni, ma sconsigliabile se abbiano intenzione di "sperimentare" ancora con il primo rilascio ufficiale di Android su un dispositivo commerciale. Un esordio non certo felice dal punto di vista qualitativo, ma che ci consente di sbizzarrirci non poco. E chissà che prossimamente non torneremo sull'argomento con qualche istruzione avanzata!

Massimiliano Basile

L'arrivo in Italia del "G1" è previsto per i primi mesi del 2009 (si parla dell'inizio della primavera).